Secure Social Internet of Things Based on Post-Quantum Blockchain

Haibo Yi

***Abstract*—With the advancement of the application of Internet of Things (IoTs), the IoT technology is combining with the social network, forming a new network with private object information as the media and social entertainment as the purpose. Social Internet of things (SIoTs) is a new application of IoT technology in social network. The current SIoT systems are centralized and the user's security and privacy is not properly protected. In order to address the challenges in SIoTs, we propose a privacy protection system for the users. First, we propose a post-quantum ring signature. Second, we propose a blockchain system based on the ring signature. Compared with the traditional SIoTs, our system is based on post-quantum techniques, which is secure against both traditional computers and quantum computers. The results of the blockchain system show that it is very suitable for SIoTs.**

***Index Terms*—Social Internet of Things (SIoTs), Internet of Things (IoTs), Blockchain, Post-Quantum Signature.**

I. Introduction

THE social Internet of Things (SIoTs) is one of the new forms of the Internet of Things (IoTs) in recent years. SIoT is a new application of IoT technology in the social network. Using the perception monitoring technology of IoTs, ordinary objects in our life can realize real-time informatization.

Social network is the relationship network between people. People are the nodes in the network, and they are organized together by the friend relationship between people. In the SIoT environment, the research scope of social network will be extended to things and things, things and people, so as to show the quantity or quantity with the general social network in the aspects of attribute, structure, content, location and so on qualitative difference.

But the SIoT faces security and privacy issues. The root cause of this problem is too centralized architecture. Using blockchain to break the centralized architecture and realize the decentralized SIoTs has become one of the research hotspots.

Blockchain is a decentralized and distributed system widely used in the area of crypto-currencies [1]–[8]. It was first conceptualized by Satoshi Nakamoto in 2008 [9]. Blockchain is designed with a growing list of blocks based on cryptographic schemes and protocols [10]. Each block in blockchain contains its transaction data, timestamp and the hash value of the previous block [11]. In addition to crypto-currencies, blockchain can be used into many other areas, e.g., smart contracts, financial services [12], [13]. Smart contracts are proposed based on blockchain that can be executed without human interaction [14]–[16]. Besides, it can be used to create a public, permanent and transparent ledger for compiling data on tracking digital use, sales and payments to content creators [17]–[30].

Motivation: Specifically, blockchain has emerged as an innovative tool for building SIoTs and other industrial applications [31]–[33]. The current SIoT systems are centralized and the user's security and privacy is not properly protected. Blockchain is decentralized without an authorized third party and there is not a trusted organization in charge of the information on blockchains [34]. Security and privacy are very vital to build blockchain system for SIoTs [35].

(1) In the design of blockchain, the information is public to everyone and the user's privacy information can be obtained by analyzing the relation between the input and output of the transactions, the determination of the output address. Thus, it is very crucial to protect the personal privacy on blockchain.

(2) Quantum computer is considered to be one of the major threats to blockchain due to the fact that the security infrastructure used in blockchain is vulnerable against the attacks on quantum computers [36]–[43]. In blockchains, it is claimed that the use of RSA and ECC cryptographic systems is not secure under quantum computer attacks.

The research of quantum computer is developing rapidly. Google has announced the realization of "quantum hegemony". In addition, enterprises and research institutions in the United States and Canada have made gratifying achievements in quantum computer research. The development of practical quantum computer will come out in the near future. Therefore, the threat of quantum computer will be an important problem to be solved. The way to resist the attack of quantum computing is to construct a mathematical problem that has no solution in quantum computer or in finite time. On this basis, the corresponding password system is constructed to protect the security of related applications.

Our contributions: In order to address the security and privacy challenges in SIoTs, we present ring signatures and post-quantum techniques to exploit blockchain system.

(1) We propose a post-quantum ring signature scheme based on multivariate polynomials for privacy protection in SIoTs. Post-quantum ring signatures can be used in many areas, such as IoT security, cloud security and etc.

Manuscript received November 22, 2020; revised May 22, 2021; accepted July 3, 2021. Date of publication July 7, 2021; date of current version May 23, 2022. This work was supported by Shenzhen Science and Technology Program under Grant 20200821082500001. Recommended for acceptance by Dr. Carlos Enrique Montenegro Marin. *(Corresponding author: Haibo Yi.)*

The author is with the School of Artificial Intelligence, Shenzhen Polytechnic, Shenzhen 518055, China (e-mail: haiboyi@szpt.edu.cn).

Digital Object Identifier 10.1109/TNSE.2021.3095192

(2) Based on the post-quantum ring signature scheme, we further propose a post-quantum blockchain for securing SIoTs.

By integrating the proposed designs, we propose a blockchain SIoT system, which is based on a new ring signature scheme that leads to a high level of anonymity. The results of the system are analyzed and future researches are discussed, which show that the proposed blockchain system is secure and efficient and is very suitable for SIoT applications. All messages from SIoTs should be uploaded to the blockchain. The message from SIoTs is signed by a group of users with the aided of post-quantum ring signature. Other users can verify the message but can not reveal the real identity of the owner of message. Then, the message and the signature are uploaded to the blockchain. The proposed design provides more security and privacy in current and quantum era.

Organization. Section II introduces the background information. Section III introduces the methodology of this paper. Section IV proposes a post-quantum ring signature scheme. Section V proposes a blockchain based on post-quantum ring signature scheme and results are analyzed. Section VI presents a blockchain system for SIoTs. Section VII summarizes our design and future researches are discussed.

II. Preliminaries

A. Blockchain and Bitcoin

Blockchain is a decentralized and distributed system widely used in the area of crypto-currencies, smart contracts, financial services and industrial applications. It was first conceptualized by Satoshi Nakamoto in 2008 and has been used in Bitcoin.

Bitcoin is a decentralized digital currency that enables instant payments to anyone, anywhere in the world, which uses peer-to-peer technology to operate with no central authority. The original Bitcoin invented by Satoshi Nakamoto was released under the MIT license, which is the first successful implementation of a distributed cryptocurrency. The transactions and emissions of Bitcoin are regulated by an extensive peer-to-peer network, which uses a distributed public universal database. The peer-to-peer network uses digital signatures and is supported by a proof-of-work protocol to ensure security and legitimacy of funds in use. To guarantee that a third-party cannot spend a user's bitcoins by issuing false transactions in their name, Bitcoin uses public key cryptography. Each person has one or more addresses or wallets, each with an associated pair of public and private keys. A user can sign a transaction with their private key, and the rest of the peers in the network can validate the signature using that users public key. Nowadays, Bitcoin is the most widespread cryptocurrency. Its total market value is over 171 billion dollars.

Blockchain is designed with a growing list of blocks based on cryptographic schemes and protocols. Each block in blockchain contains its transaction data, timestamp and the hash value of the previous block. The security infrastructure used in blockchain is ECC cryptographic system, which is claimed to be not secure under quantum attacks.

B. Quantum Computer Threats to Blockchain

Quantum computers are one of the future major computers that built on quantum entities such as photons, electrons, atoms and ions. Compared with traditional computers, they run quantum bits and have parallel processing ability based on quantum bits. Theoretically, the computing ability of quantum computers increases with the increase of their quantum bits. Thus, quantum computers have very powerful computing ability.

In recent years, Google, IBM, Microsoft and other large companies have invested in the development of hardware and software for quantum computers. In 2017, IBM announced the development of a quantum computer prototype with 50 quantum bits. In 2018, Google released 72 quantum bits of quantum chip and Microsoft announced that it had significant progress in the development of topological quantum computing.

Quantum computers are considered to pose a major security threat to the cryptographic systems currently in use. Blockchains mainly rely on elliptic curve public key cryptography algorithm to generate digital signatures for secure transactions. In public key cryptographic area, the most commonly used cryptographic schemes, such as ECDSA, RSA, DSA, can not resist quantum attacks in theory. Although asymmetric elliptic curve cryptography encryption with a certain length private keys is secure and must be broken by super computers using dozens of years, according to theoretical prediction, Shor algorithms that runs on thousand bits quantum computers are expected to broke such encryption in dozens of minutes.

Quantum algorithms will seriously affect the public key cryptographic systems currently used in blockchains. We must propose security strategies to deal with such challenges in blockchains.

C. Privacy Protection in Blockchain

In the design of blockchain, the transaction information is public to everyone and the user's privacy information can be obtained by analyzing the the relation between the input and output of the transactions, the determination of the output address. Thus, it is very crucial to protect the personal privacy on blockchain.

D. Post-Quantum Cryptography

In order to deal with the security threat of quantum computer to blockchains, two main countermeasures are quantum cryptography and post-quantum cryptography.

Quantum cryptography is the future cryptography that runs on quantum computers. It performs cryptographic tasks by exploiting quantum mechanical properties. One of the famous example of quantum cryptography is quantum key distribution. It offers a secure solution of information theory to the key exchange problem. Potentially, quantum key distribution has higher security based on physics compared with traditional cryptography, but the main disadvantage lies in the fact that quantum hardware systems are very expensive, which is not conducive to rapid and large-scale applications.

Post-quantum cryptography is based on certain mathematical problems that can not be accelerated by quantum computers. Thus, it is considered to be secure to quantum computers. In 2006, the first post-quantum cryptography conference was held. Since then, many organizations, enterprises and research groups have used such mathematical problems to design post-quantum cryptographic schemes. At present,

multivariate cryptography, lattice-based cryptography, hash-based cryptography and code-based cryptography are considered to be the main candidates of post-quantum cryptography. Such cryptographic schemes can resist quantum computer attacks with enough long private keys.

E. Multivariate Cryptography

Among post-quantum cryptography, multivariate cryptography is one of the popular candidates for building the next generation blockchain. Multivariate schemes include Rainbow, UOV, enTTS, Simplematrix, and etc. The security of multivariate cryptography is based on a NP-hard problem, i.e., solving multivariate quadratic equations. The core of multivariate equations is multivariate quadratic polynomials, which includes multivariate variables and coefficients.

The main functions to build a multivariate scheme are central map transformation and affine transformation.

(1) Central map transformation: it is a set of multivariate equations on Vinegar variables and Oil variables in a finite field. The central map transformation is to solve the Oil variables. Generally, central map transformation includes multiple layers. On the first layer, the Vinegar variables are randomly generated. The Vinegar variable of the lower layer is the Vinegar variables and Oil variables of the upper layer.

(2) Affine transformation: it is a transformation performed by matrix-vector multiplication and vector addition in a finite field.

F. Ring Signature

Ring signature is a type of special digital signatures, which was invented in 2001. Compared with traditional signatures, ring signature can be generated by any member from a group of users that each have a set of private keys and public keys. Generally, any member from a group of users signs a message by using his/her private key and other member's public keys. The ring signature can be verified by the public and the only information known to the public is the signature is signed from a group of users. Thus, the identity of the user who signs the ring signature is concealed in a group of users.

Ring signature is very suitable to design private protection system in blockchain. Via using ring signature, people only knows that transaction is made from a group of users and the user who makes the transaction remains anonymous. Most ring signature schemes currently used are based on RSA and ECC. However, they are claimed to be not secure against quantum computer attacks. Fortunately, there are four main public key cryptographic schemes are considered to be secure against quantum computer attacks.

III. Methodologies

We present ring signatures and post-quantum techniques to exploit blockchain system.

First, in order to improve privacy protection in SIoTs, we propose a post-quantum ring signature scheme based on multivariate polynomials.

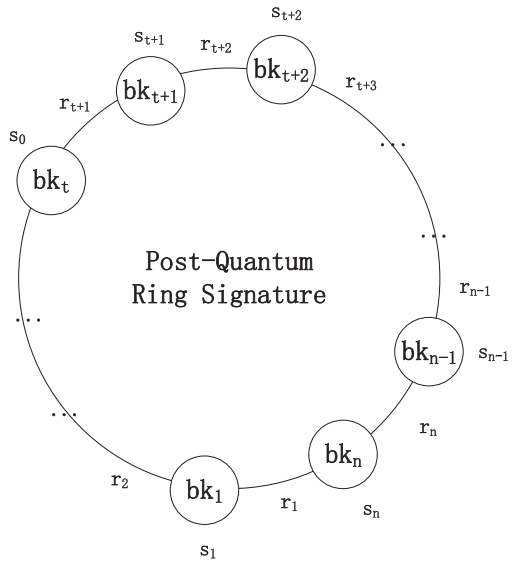

Fig. 1. Post-Quantum Ring Signature.

(1) The security of our ring signature scheme is based on a NP-hard problem, i.e., solving multivariate quadratic equations. The form of the quadratic equations is as follows, where O and V are variables, a, b, c, d are coefficients, and e is constant.

$$y = a_{ij}O_iV_j + b_{ij}V_iV_j + c_iO_i + d_iV_i + e.$$

(2) We assume that a group has n users with sets of private keys and public keys, i.e., vk_i and bk_i, where $i = 1, 2, \ldots, n$.

(3) Each user from a group has a set of private key and public key.

(4) Private keys are generated randomly and public keys are computed based on private keys.

(5) The generations of private keys and public keys are described in Section IV-F.

(6) The t-th user from the group needs to generate a ring signature of message m.

(7) We depict the scheme in Fig. 1. Public keys of the users from the group and the private key of the user who sings the ring signature are composed of a ring.

(8) We summary the scheme in Table I. The private keys used in post-quantum ring signature scheme are vk_t, s_0, where vk_t is the private key of the t-th user and s_0 is a random variable. The public key used in post-quantum ring signature scheme are $bk_1, bk_2, \ldots, bk_n$, which are the public keys of n users respectively.

(9) Post-quantum ring signatures can be used in many areas, such as IoTs security, cloud security and etc.

Second, we further propose a post-quantum blockchain for securing SIoTs based on the post-quantum ring signature scheme.

(1) The blockchain network nodes are divided into several groups.

(2) Each group has n blockchain network node users with sets of private keys and public keys, i.e., vk_i and bk_i, where $i = 1, 2, \ldots, n$.

(3) Each user from a group has a set of private key and public key. Private keys are generated randomly and public keys are computed based on private keys.

TABLE I
POST-QUANTUM RING SIGNATURE SCHEME

Message	Signature	Private Keys	Public Keys	Main Functions	Finite Field
m	$r_1, s_1, s_2, ..., s_n$	vk_t, s_0	$bk_1, bk_2, ..., bk_n$	$L, F, \bar{F}, P_1, P_2$	$GF(2^8)$

(4) If the t-th user from the group needs to submit a transaction to the blockchain, he use the private keys of the group to generate a ring signature of the transaction.

(5) The transaction looks like be signed by a group of users. Thus, the privacy protection is improved.

(6) The security of the system is based on post-quantum techniques, which is secure against both traditional computers and quantum computers.

Third, based on above designs, we propose a blockchain system and discuss its applications to secure SIoTs.

IV. POST-QUANTUM RING SIGNATURE SCHEME

A. Overview of the Post-Quantum Ring Signature Scheme

Tn order to improve privacy protection in SIoTs, we propose a post-quantum ring signature scheme based on multivariate polynomials.

We assume that a group has n users with sets of private keys and public keys, i.e., vk_i and bk_i, where $i = 1, 2, \ldots, n$. Each user from a group has a set of private key and public key. Private keys are generated randomly and public keys are computed based on private keys. Public keys of the users from the group and the private key of the user who sings the ring signature are composed of a ring.

If the t-th user from the group needs to generate a ring signature of message m and the public needs to verify the ring signature, we present post-quantum ring signature generation and verification in Section IV-B.

(1) Affine transformation and central map transformation are described in Section IV-C and Section IV-D, which are the main functions of signature generation.

(2) Multivariate polynomial evaluation is described in Section IV-E, which is the main function of signature verification.

(3) The generations of private keys and public keys are described in Section IV-F.

(4) Other functions designed in post-quantum ring signature scheme are P_1 and P_2, which are described in Section IV-G.

(5) We analyse the anonymity and security of the post-quantum ring signature in Section IV-H.

B. Post-Quantum Ring Signature Generation and Verification

Ring Signature Generation. First, it is required to generate random values $s_0, s_1, \ldots, s_{t-1}, s_{t+1}, s_{t+2}, \ldots, s_n$.

Second, we compute the following equation.

$r_{t+1} = \bar{F}(bk_t, P_1(M, bk_1, bk_2, \ldots, bk_n, s_0))$.

$\bar{F}$ is a function of multivariate polynomial evaluation as described in Section IV-E. P_1 is a function as described in Section IV-G.

Second, we compute the following equations for $i = t+2$, $t+3, \ldots, n$.

$r_i = \bar{F}(bk_{i-1}, P_1(M, bk_1, bk_2, \ldots, bk_n, s_{i-1})) + \bar{F}(bk_{i-1}, P_2(r_{i-1}))$.

P_2 is a function as described in Section IV-G.

Third, we compute the following equation.

$r_1 = \bar{F}(bk_n, P_1(M, bk_1, bk_2, \ldots, bk_n, s_n)) + \bar{F}(bk_n, P_2(r_n))$.

Fourth, we compute the following equations for $i = 2, \ldots, t$.

$r_i = \bar{F}(bk_{i-1}, P_1(M, bk_1, bk_2, \ldots, bk_n, s_{i-1})) + \bar{F}(bk_{i-1}, P_2(r_{i-1}))$.

After that, $r_1, r_2, \ldots, r_n$ are computed. Then, we compute s_t based on the following equation.

$\bar{F}(bk_t, P_1(M, bk_1, bk_2, \ldots, bk_n, s_t)) = \bar{F}(bk_t, P_1(M, bk_1, bk_2, \ldots, bk_n, s_0)) - \bar{F}(bk_t, P_2(r_t))$.

In order to compute s_t, we compute the following equation.

$cons = \bar{F}(bk_t, P_1(M, bk_1, bk_2, \ldots, bk_n, s_0)) - \bar{F}(bk_t, P_2(r_t))$.

Then, we use the private key of the t-th user to compute the following equation.

$P_1(M, bk_1, bk_2, \ldots, bk_n, s_t) = L \circ F(vk_t, cons)$.

F is a function of central map transformation as described in Section IV-D. L is an affine transformation as described in Section IV-C.

Finally, we compute s_t from function P_1 and the ring signature for message m is $(r_1, s_1, s_2, \ldots, s_n)$.

Ring Signature Verification. In order to verify a ring signature $(r_1, s_1, s_2, \ldots, s_n)$ for message m, we compute the following equations for $i = 2, 3, \ldots, n$.

$r_i = \bar{F}(bk_{i-1}, P_1(M, bk_1, bk_2, \ldots, bk_n, s_{i-1})) + \bar{F}(bk_{i-1}, P_2(r_{i-1}))$.

After that, $r_2, \ldots, r_n$ are computed. Then, we compute the following equation.

$r'_1 = \bar{F}(bk_n, P_1(M, bk_1, bk_2, \ldots, bk_n, s_n)) + \bar{F}(bk_n, P_2(r_n))$.

If $r'_1 = r_1$, the ring signature is verified. Otherwise, we reject the signature.

We analyze the security of the ring signature scheme in Section IV-H.

C. Affine Transformation

The function L designed in post-quantum ring signature scheme is affine transformation in finite field $GF(2^8)$, which is illustrated in Table II, where private keys A, B are involved and A is a matrix with size of 56×56 and B is a vector with size of 56. We performed affine transformation as follows.

$L : y = Ax + B$.

The function $L(x)$ is performed with two steps, where x is a with size of 56.

First, $A' = Ax$ is performed as matrix-vector multiplication in finite field $GF(2^8)$.

Second, $y = A' + B$ is performed as vector addition in finite field $GF(2^8)$.

In function L, matrix A and vector B are private keys.

D. Central Map Transformation

The function F designed in post-quantum ring signature scheme is central map transformation in finite field $GF(2^8)$,

TABLE II
AFFINE TRANSFORMATION FUNCTION

Function	Input	Output	Input Size	Output Size	Private Keys	Finite Field
L	x	y	56 Bytes	56 Bytes	A, B	$GF(2^8)$

TABLE III
CENTRAL MAP TRANSFORMATION FUNCTION

Function	Input	Output	Input Size	Output Size	Private Keys	Finite Field
F	y	$O_1, O_2, ..., O_{28}, V_1, V_2, ..., V_{28}$	28 Bytes	56 Bytes	$\alpha, \beta, \chi, \delta, \varepsilon, V$	$GF(2^8)$

TABLE IV
MULTIVARIATE POLYNOMIAL EVALUATION FUNCTION

Function	Input	Output	Input Size	Output Size	Public Keys	Finite Field
$\bar{F}$	$x_1, x_2, ..., x_{56}$	y	56 Bytes	28 Bytes	ϕ, φ, γ	$GF(2^8)$

which is illustrated in Table III, where private keys $\alpha, \beta, \chi, \delta, \varepsilon, V$ are coefficients. We performed central map transformation as follows.

Central map transformation includes 28 multivariate polynomials with the following form.

$\sum \alpha_{ij} O_i V_j + \sum \beta_i O_i + \sum \chi_{ij} V_i V_j + \sum \delta_i V_i + \varepsilon$.

$O_1, O_2, \ldots, O_{28}$ is 28 Oil variables in finite field $GF(2^8)$, which is required to be solve. $V_1, V_2, \ldots, V_{28}$ is 28 Vinegar variables in finite field $GF(2^8)$, which is randomly chosen during each central map transformation.

Then, we compute $F(O) = y$, where y is the input with 28 variables in finite field $GF(2^8)$.

Next, we generate $V_1, V_2, \ldots, V_{28}$ randomly and substitute them into $F(O) = y$.

Then, $F(O) = y$ is transformed to systems of linear equations on variables $O_1, O_2, \ldots, O_{28}$.

Finally, we solve the systems of linear equations and get $O_1, O_2, \ldots, O_{28}$.

$O_1, O_2, \ldots, O_{28}$ and $V_1, V_2, \ldots, V_{28}$ are the output.

In function F, $\alpha, \beta, \chi, \delta, \varepsilon, V$ are private keys.

E. Multivariate Polynomial Evaluation

The function $\bar{F}$ designed in post-quantum ring signature scheme is multivariate polynomial evaluation in finite field $GF(2^8)$, which is illustrated in Table IV and performed as follows.

Multivariate polynomial evaluation includes 28 multivariate polynomials with the following form.

$\sum \phi_{ij} x_i x_j + \sum \varphi_i x_i + \gamma$.

$x_1, x_2, \ldots, x_{56}$ are 56 inputs in finite field $GF(2^8)$.

Then, we compute $\bar{F}(x) = y$, where y is the outputs with 28 variables in finite field $GF(2^8)$.

In function F, ϕ, φ, γ are public keys.

F. Private Keys and Public Keys Generation

Private keys and public keys generation designed in post-quantum ring signature scheme is illustrated in Table V and performed as follows.

TABLE V
PRIVATE KEYS AND PUBLIC KEYS

Private Keys	Public Keys
$\alpha, \beta, \chi, \delta, \varepsilon, V, A, B$	ϕ, φ, γ

Private Keys Generation. For private keys $\alpha, \beta, \chi, \delta, \varepsilon, V, A, B$, they are generated randomly in finite field $GF(2^8)$.

Public Keys Generation. Private keys $\alpha, \beta, \chi, \delta, \varepsilon, V$ are substituted into F and A, B are substituted into L.

Then, public keys ϕ, φ, γ are computed based on $\bar{F} = L \circ F$.

G. Other Functions

Other functions designed in post-quantum ring signature scheme are P_1 and P_2.

P_1 Function. The function P_1 designed in post-quantum ring signature scheme is illustrated in Table VI and performed as follows.

The input of P_1 is $M, bk_1, bk_2, \ldots, bk_n, s_i$.

First, we compute the hash value of $M|bk_1|bk_2|\ldots|bk_n|s_i$ based on SHA-512 algorithm and get the hash value h.

Second, we use h' to denote the first 40 bytes of h.

Last, we output $y = s_i|h'$.

P_2 Function. The function P_2 designed in post-quantum ring signature scheme is illustrated in Table VII and performed as follows.

The input of P_1 is r_i.

First, we compute the hash value of r_i based on SHA-512 algorithm and get the hash value h.

Second, we use h' to denote the first 56 bytes of h.

Last, we output $y = h'$.

H. Security Analysis

We analyse the anonymity and security of the post-quantum ring signature scheme as follows.

(1) The ring signature verification uses all users' public keys from a group. Thus, the user who signs the signature is anonymous.

TABLE VI
P_1 FUNCTION

Function	Input	Output	Input Size	Output Size	Finite Field
P_1	$M, bk_1, bk_2, ..., bk_n, s_i$	y	No Limit	56 Bytes	$GF(2^8)$

TABLE VII
P_2 FUNCTION

Function	Input	Output	Input Size	Output Size	Finite Field
P_2	r_i	y	28 Bytes	56 Bytes	$GF(2^8)$

(2) Attackers only have the signature $(r_1, s_1, s_2, \ldots, s_n)$ and all users' public keys. The difficulty to obtain the private keys relies on the NP-hard problem, i.e., solving quadratic equations, which is considered to be secure to traditional computer attacks and quantum computer attacks.

(3) If attackers want to fake a ring signature, they need to find s_t when $P_1(M, bk_1, bk_2, \ldots, bk_n, s_t) = L \circ F(vk_t, cons)$ is workable. s_t is a 16-byte variable. Thus, the brute-force attack is 2^{128}.

Compared with the other ring signatures, such as RSA ring signature and ECC ring signature, the post-quantum ring signature is able to resist both traditional computer attacks and quantum computer attacks.

V. BLOCKCHAIN SIOTS

A. Overview of the Blockchain SIoTs

In the design of blockchain, the transaction information is public to everyone and the user's privacy information can be obtained by analyzing the the relation between the input and output of the transactions, the determination of the output address. Thus, it is very crucial to protect the personal privacy on blockchain. We further propose a blockchain for securing SIoTs based on the post-quantum ring signature scheme. Compared with the original blockchain, the improvement is illustrated as follows.

(1) The blockchain network users are divided into several groups.

(2) Each group is assigned to a group ID.

(3) Each user is assigned to a user ID and maintains a full copy of blockchain. The real identity of the user is anonymous.

(4) Each group has n blockchain network node users with sets of private keys and public keys, i.e., vk_i and bk_i, where $i = 1, 2, \ldots, n$.

(5) Each group has a set of group private key and public key.

(6) Each user submits the transaction by using the group ID and the group signature.

The actions of user look like the actions of a group. Thus, the privacy protection of blockchain is improved. The security of blockchain is based on post-quantum techniques, which is secure against both traditional computers and quantum computers.

B. Blockchain Network

The new blockchain is maintained by a blockchain network with a certain number of nodes. We illustrate the blockchain network as follows.

(1) The nodes of the blockchain network are divided into several groups.

(2) Each group has n blockchain network nodes.

(3) Each node represents a user.

(4) Each user from a group has a set of private key and public key.

(5) Private keys are generated randomly and public keys are computed based on private keys.

(6) When a new node joins the blockchain network, it is assigned to a random group with user number less than n.

(7) When a node leaves the blockchain network, it is removed from the group.

(8) Before new blocks of blockchain generate, groups of nodes of the blockchain network are regenerated.

C. Blockchain

Each user maintains a full copy of blockchain. Compared with the traditional blockchain, the improvement is illustrated as follows.

(1) Each transaction is submitted by a group of users. Thus, it is very difficult to reveal the real transaction submitter.

(2) Each block is generated by a group of users. Thus, it is very difficult to reveal the real block generator.

D. Transaction Submission on Blockchain

If the t-th user from the group needs to submit a transaction to the blockchain, he use the private keys of the group to generate a ring signature of the transaction M.

(1) We suppose that the users' public keys from a group of n users are bk_i, where $i = 1, 2, \ldots, n$. The t-th user's private key is vk_t.

(2) Random values $s_0, s_1, \ldots, s_{t-1}, s_{t+1}, s_{t+2}, \ldots, s_n$ are generated.

(3) The following computation is performed.

$r_{t+1} = \bar{F}(bk_t, P_1(M, bk_1, bk_2, \ldots, bk_n, s_0))$.

(4) For $i = t+2, t+3, \ldots, n$, the following computation is performed.

$r_i = \bar{F}(bk_{i-1}, P_1(M, bk_1, bk_2, \ldots, bk_n, s_{i-1})) + \bar{F}(bk_{i-1}, P_2(r_{i-1}))$.

(5) The following computation is performed.

$r_1 = \bar{F}(bk_n, P_1(M, bk_1, bk_2, \ldots, bk_n, s_n)) + \bar{F}(bk_n, P_2(r_n))$.

(6) For $i = 2, 3, \ldots, t$, the following computation is performed.

$r_i = \bar{F}(bk_{i-1}, P_1(M, bk_1, bk_2, \ldots, bk_n, s_{i-1})) + \bar{F}(bk_{i-1}, P_2(r_{i-1}))$.

TABLE VIII
COMPARISONS WITH THE RELATE SYSTEMS

System	Architecture	Security	Efficiency	Privacy Protection
Our SIoT System	Decentralized	High	Moderate	High
Blockchain SIoT System	Decentralized	Moderate	Moderate	Moderate
SIoT System	Centralized	Low	High	Low

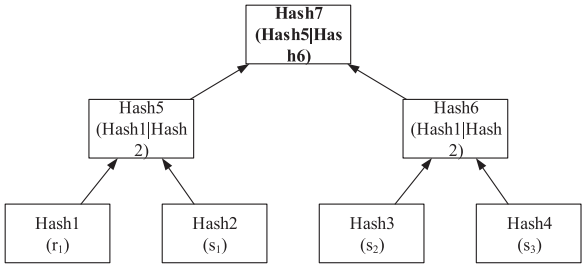

Fig. 2. Ring Signature Tree.

(7) $r_1, r_2, \ldots, r_n$ are computed. s_t is computed based on the following equation.

$\bar{F}(bk_t, P_1(M, bk_1, bk_2, \ldots, bk_n, s_t)) = \bar{F}(bk_t, P_1(M, bk_1, bk_2, \ldots, bk_n, s_0)) - \bar{F}(bk_t, P_2(r_t))$.

(8) In order to compute s_t, the following computation is performed.

$cons = \bar{F}(bk_t, P_1(M, bk_1, bk_2, \ldots, bk_n, s_0)) - \bar{F}(bk_t, P_2(r_t))$.

(9) The private key of the t-th user is used to perform the following computation.

$P_1(M, bk_1, bk_2, \ldots, bk_n, s_t) = L \circ F(vk_t, cons)$.

(10) s_t is computed from function P_1 and the ring signature for the transaction m is $(r_1, s_1, s_2, \ldots, s_n)$.

$(r_1, s_1, s_2, \ldots, s_n)$ is stored in blockchain as ring signature tree, which is depicted Fig. 2. The leaf of ring signature tree is the hash of each value from $(r_1, s_1, s_2, \ldots, s_n)$. We combine two hash values and compute their hash value as the value of their father. By computing the similar operations in each layer of ring signature tree, the tree root is computed. If any value from $(r_1, s_1, s_2, \ldots, s_n)$ is changed, the root will be changed. The user can only store the value of tree root to reduce the storage requirement.

The other users want to verify the ring signature $(r_1, s_1, s_2, \ldots, s_n)$ for transaction m, they obtain the users' public keys from a group, i.e., bk_i, where $i = 1, 2, \ldots, n$. Then, they verify the signature based on the post-quantum ring signature verification.

(1) For $i = 2, 3, \ldots, n$, the following computation is performed.

$r_i = \bar{F}(bk_{i-1}, P_1(M, bk_1, bk_2, \ldots, bk_n, s_{i-1})) + \bar{F}(bk_{i-1}, P_2(r_{i-1}))$.

(2) After that, $r_2, \ldots, r_n$ are computed by the similar method.

(3) Then, the following computation is performed.

$r'_1 = \bar{F}(bk_n, P_1(M, bk_1, bk_2, \ldots, bk_n, s_n)) + \bar{F}(bk_n, P_2(r_n))$.

(4) If $r'_1 = r_1$, the ring signature is verified. Otherwise, the signature is rejected.

The process of the other users verify the signature of transaction can not reveal the real identity of the transaction submitter. Thus, the anonymity of the blockchain is improved.

VI. BLOCKCHAIN SYSTEM FOR SIOTS

A. Overview of Blockchain System

In order to address such challenges, we exploit the blockchain technology to propose a blockchainsystem for SIoTs. The blockchainsystem can be widely used in many scenarios.

B. Blockchain

The blockchain is maintained by users, i.e., sellers, buyers and IoT users.

(1) Sellers: they maintain nodes with surplus electricity and energy to sell.

(2) Buyers: they maintain nodes with electricity and energy demand.

(3) IoT users: they maintain nodes that supply the IoT services.

C. Payment

Sellers and buyers have electricity and energy coins that stored in their wallets. A buyer uses the group ID to transfer the coins from his wallet to a industrial seller's wallet with a transaction signed by a group of users.

(1) The transaction's signature verification uses all users' public keys from a group. Thus, the industrial buyer who signs the signature is anonymous.

(2) Attackers only have the signature and all industrial buyers' public keys. The difficulty to obtain the private keys of industrial buyers relies on the NP-hard problem, i.e., solving quadratic equations, which is considered to be secure to traditional computer attacks and quantum computer attacks.

(3) If attackers want to fake a transaction signature, they need to find a unmown 16-byte variable and the brute-force attack is 2^{128}.

As shown in Table VIII, compared with the other system, the blockchain system provides a higher level of anonymity and post-quantum security.

VII. CONCLUSIONS

Security and privacy are very vital to blockchain system for SIoTs. We propose a post-quantum ring signature scheme based on multivariate polynomials for privacy protection. Based on the post-quantum ring signature scheme, we further propose a post-quantum blockchain for securing SIoTs. By integrating the proposed designs, we propose a blockchain system. We exploit the blockchain technology to propose a blockchain system for SIoTs. All messages from SIoTs should be uploaded to the blockchain.

The message from SIoTs is signed by a group of users with the aided of post-quantum ring signature. Other users can verify the message but can not reveal the real identity of the owner of message. Then, the message and the signature are uploaded to the blockchain. Besides, the blockchain system can be widely used in many other scenarios.

REFERENCES

[1] J. Xu, S. Wang, and B. K. Bhargava, "A Blockchain-enabled trustless crowd-intelligence ecosystem on mobile edge computing," *IEEE Trans. Ind. Inform.*, vol. 15, no. 6, pp. 3538–3547, Jun. 2019.

[2] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *J. Med. Syst.*, vol. 43, no. 1, pp. 1–9, 2019.

[3] Z. Xiong, Z. Yang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, U.S., vol. 56, no. 8, pp. 33–39, Aug. 2018.

[4] Z. Li *et al.*, "Does bitcoin bubble burst?," *Qual. Quantity*, vol. 53, no. 1, pp. 91–105, 2019.

[5] R. Beck, "Beyond bitcoin: The rise of blockchain world," *Computer*, vol. 51, no. 2, pp. 54–58, 2018.

[6] A. Maxmen, "AI researchers embrace bitcoin technology to share medical data," *Nature*, vol. 555, no. 7696, pp. 293–294, 2018.

[7] S. Lahmiri, and S. Bekiros, "Chaos, randomness and multi-fractality in bitcoin market," *Chaos Solitons Fractals*, vol. 106, pp. 28–34, 2018.

[8] I. Giechaskiel, C. Cremers, and B. Rasmussen, "When the crypto in cryptocurrencies breaks: Bitcoin security under broken primitives," *IEEE Secur. Privacy*, vol. 16, no. 4, pp. 46–56, Jul./Aug. 2018.

[9] P. Treleaven, G. Brown, and D. Yang, "Blockchain technology in finance," *Computer*, vol. 50, no. 9, pp. 14–17, 2017.

[10] A. Dorri, M. Steger, S. Kanhere, and R. Jurdak, "Blockchain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, U.S., vol. 55, no. 12, 119–125, Dec. 2017.

[11] T. Aste, P. Tasca, and D. Matteo, "Blockchain technologies: The foreseeable impact on society and industry," *Computer*, vol. 50, no. 9, pp. 18–28, 2017.

[12] P. Dunphy, and P. A. Petitcolas, "First look at identity management schemes on the blockchain," *IEEE Secur. Privacy*, vol. 16, no. 4, pp. 20–29, Jul./Aug. 2018.

[13] S. Wu, Y. Chen, Q. Wang, M. Li, C. Wang, and X. Luo, "CReam: A. smart contract enabled collusion-resistant e-auction," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 7, pp. 1687–1701, Jul. 2019.

[14] D. Magazzeni, P. Mcburney, and W. Nash, "Validation and verification of smart contracts: A research agenda," *Computer*, vol. 50, no. 9, pp. 50–57, 2017.

[15] N. Griggs *et al.*, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *J. Med. Syst.*, vol. 42, no. 7, pp. 1–7, 2018.

[16] K. Hara, "Smart contracts - Dumb idea," *IEEE Internet Comput.*, vol. 21, no. 2, 97–101, Mar./Apr. 2017.

[17] V. Gatteschi *et al.*, "To blockchain or not to blockchain: That is the question," *IT Professional*, vol. 20, no. 2, pp. 62–74, 2018.

[18] H. Orman, "Blockchain: The emperors new PKI?" *IEEE Internet Comput.*, vol. 22, no. 2, pp. 23–28, Mar./Apr. 2018.

[19] J. Hou, H. Wang, and P. Liu, "Applying the blockchain technology to promote the development of distributed photovoltaic in China," *Int. J. Energy Res.*, vol. 42, no. 6, pp. 2050–2069, 2018.

[20] C. Pop *et al.*, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 2, pp. 1–21, 2018.

[21] K. Gammon, "Experimenting with blockchain: Can one technology boost both data integrity and patients' pocketbooks?," *Nat. Med.*, vol. 24, no. 4, pp. 378–381, 2018.

[22] L. Mertz, "Hospital CIO explains blockchain potential: An interview with beth israel deaconess medical center's john halamka," *IEEE Pulse*, vol. 9, no. 3, pp. 8–19, May/Jun. 2018.

[23] N. Khaqqi *et al.*, "Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application," *Appl. Energy*, vol. 209, pp. 8–19, 2018.

[24] Z. Aitzhan, and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 840–852, Sep.-Oct. 2018.

[25] G. Feng, L. Zhu, S. Meng, K. Sharif, Z. Wan, and K. Ren, "A Blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE Netw.*, vol. 32, no. 6, pp. 184–192, Nov./Dec. 2018.

[26] F. Kai *et al.*, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G," *IET Commun.*, vol. 12, no. 5, pp. 527–532, 2018.

[27] G. Liang, R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Distributed blockchain-based data protection framework for modern power systems against cyber attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3162–3173, May 2019.

[28] O. Malomo, B. Rawat, and M. Garuba, "Next-generation cybersecurity through a blockchain-enabled federated cloud framework," *J. Supercomputing*, vol. 74, no. 10, pp. 5099–5126, 2018.

[29] Chien-Ming Chen, and B. Xiang, "Yining liu and king-hang wang. a. secure authentication protocol for Internet of Vehicles, *IEEE Access*, vol. 7, no. 1, pp. 12047–12057, Dec. 2019.

[30] Chien-Ming Chen, B. Xiang, King-Hang Wang, Kuo-Hui Yeh, and Tsu-Yang Wu, "A Robust mutual authentication with a key agreement scheme for session initiation protocol," *Appl. Sci.*, vol. 8, no 10, pp. 1–15, Oct. 2018

[31] W. Cheng, W. Wei, J. Wang, L. Wu, and Y. Liang, "Equilibrium of interdependent gas and electricity markets with marginal price based bilateral energy trading," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4854-4867, Sep. 2018.

[32] D. Mccoy, and S. Lyons, "Unintended outcomes of electricity smart-metering: Trading-off consumption and investment behaviour," *Energy Efficiency*, vol. 10, no. 2, pp. 1–20, 2017.

[33] C. Lin, J. Deng, C. Kuo, and Y. Liang, "Optimal charging control of energy storage and electric vehicle of an individual in the internet of energy with energy trading," *IEEE Trans. Ind. Inform.*, vol. 14, no. 6, pp. 2570–2578, Jun. 2018.

[34] L. Jiao, "Data transmission scheme considering node failure for blockchain," *Wireless Pers. Commun.*, vol. 103, no. 1, pp. 179–194, 2018.

[35] K. Ghassan, and Srdjan C, "Blockchain security and privacy," *IEEE Secur. Privacy*, vol. 16, no. 4, pp. 11–12, 2018.

[36] K. Fedorov, O. Kiktenko, and I. Lvovsky, "Quantum computers put blockchain security at risk," *Nature*, vol. 563, no. 7732, pp. 465–467, 2018.

[37] H. Chang, W. Yang, and T. Hwang, "Trojan horse attack free fault-tolerant quantum key distribution protocols using GHZ states," *Int. J. Theor. Phys.*, vol. 55, no. 9, pp. 1–12, 2016.

[38] Y. Wei, Y. Wang, and F. Gao, "Practical quantum private query with better performance in resisting joint-measurement attack," *Phys. Rev. A.*, vol. 93, no. 4, pp. 1–5, 2016, Art. no. 042318.

[39] Y. Wang, H. Zhang, and H. Wang, "Quantum polynomial-time fixed-point attack for RSA," *China Commun.*, vol. 15, no. 2, pp. 25–32, 2018.

[40] Y. Fei *et al.*, "Quantum man-in-the-middle attack on the calibration process of quantum key distribution," *Sci. Rep.*, vol. 8, no. 1, pp. 1–10, 2018.

[41] C. Hao, and W. Ma, "Multi-party traveling-mode quantum key agreement protocols immune to collusive attack," *Quantum Inform. Process.*, vol. 17, no. 9, pp. 1–14, 2018.

[42] M. Wustmans, T. Haubold, and B. Bruens, "Bridging trends and patents: Combining different data sources for the evaluation of innovation fields in blockchain technology," *IEEE Trans. Eng. Manag.*, vol. 69, no. 3, pp. 825–837, Mar. 2022.

[43] Y. Zhu, W. Song, D. Wang, D. Ma, and W. C. -C. Chu, "TA-SPESC: Toward asset-driven smart contract language supporting ownership transaction and rule-based generation on blockchain," *IEEE Trans. Rel.*, vol. 70, no. 3, pp. 1255–1270, Sep. 2021.

Haibo Yi received the bachelor's degree in computer science from Beijing Jiaotong University, Beijing, China, in 2009 and the Ph.D. degree from the South China University of Technology, Guangzhou, China, in 2015. Since 2015, he has been with the School of Computer Engineering, Shenzhen Polytechnic, Shenzhen, China, as an Associate Professor. He has authored or coauthored more than 20 technical papers. His main research interests include information security, cloud computing, and big data. He is a Member of Chinese Association for Cryptologic Research.